

- Bootcamp CCNA -

todo lo que quieras preguntar
contactar a Frank

1 semana - 2 bootcamps ICND 1, 2

"haciendo abierto" - Frank

"se esperan muchos cambios"

✓ Cisco x Frank property
ES un examen, NO super-coaching sit here.

ES un examen.

Frank NO es cualquier profesor

frango3@cisco.com - Frank Gonzalez

hasta las 23:00 - 55 79 40 98 72
70

"ARS" - rumbos de gamma alta

o lo domine

o NO lo domine

o NO lo habría visto :-)

- yeah it's gonna be hard

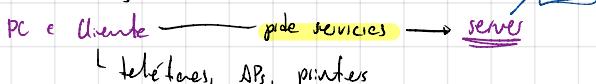
CCNA-X - 3900 USD v.3.0 - aprovechalo! >!

- veremos un montón de cosas (?) → mejor goal

↳ veremos lo básico y de dónde seguir juntando

Modelo cliente servidor

- en la vida y en las redes



↳ teléfonos, APs, impresoras

el servicio más importante? → bluh, una IP

Client ← depende → Server relación complicada

→ DHCP — necesitamos una IP antes que nada

↳ can be hosted on < tanto > servers

→ debes tener al menos 2 en la red p/q/ esto se cumpla

→ switch AKA commutador → selecciona, enruta

no temas preguntarle a Google

commutador (switch) - establece vías de comunicación

ruter AKA encaminador - te dice qué camino usar para enviar el paquete

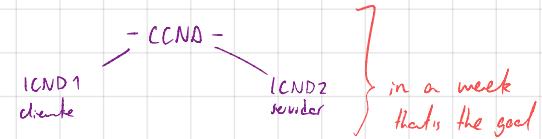
Frank explica el porqué de las cosas



SDN - sw defined networks (future model)

↳ vivimos una sw defined life, la verdad, en todo aspecto

↳ por qué la red no?



→ estructura el modelo (-s)

↳ we haremos redes eficientes :o) el scope

- qualcheinda preguntar en el momento

- Si, la red es cosa nostra

↳ reglas → protocolos → aplicación

red - elementos o devices ql se interconectan usando un medio físico cuya comunicación está gobernada por un tipo de protocolos y se encuentra limitada por su área de alcance

LAN - área NO geográfica

↳ área de alcance - m LAN

↳ NO tiene que ser el mismo edificio/grupo - idea errónea

- el modelo jerárquico / 3-tier / por capas -

/ AKA backbone

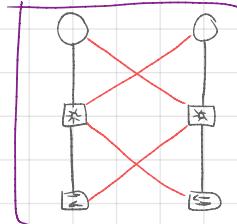
Core enlaza recursos al otros recursos

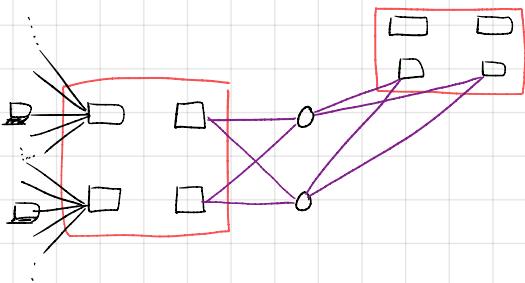
Distrib distribuye network resources

Access acceso a la red

- si se pierde un enlace, se pierde la conexión al todo

↳ redundancia → replicar todo e interconectar





- user se conecta a un device de acceso
- └ ese se va a un device de distribución
- └ ese se va a un core

todo en un building

- └ podemos tener blocks por piso en el building

IDF (room)

- └ intermedio distrib. frame

- ... y el core conecta edificios con edificios \Rightarrow Campus

(MDF, NNF)

Security / means prevention

└ prevention, más nada - NO es para mitigar

└ lógica / física

└ reglas pt operar el elemento físico: políticas de seguridad

Scalability

└ capacidad de growth/expansion

└ BUT, tech is evolving quick

└ aceptar elementos nuevos o existentes

Availability

└ es medible

└ amount of time network is available

Reliability

└ POV de quien administra la red

└ si Availability satisfies my criterion for reliability \rightarrow i'm golden

└ \Rightarrow I can tell I have a highly reliable network

Campus

múltiples edificios en la zona

encuentran en core

un edificio \Rightarrow 2-tier AKA collapsed core



PDU - NOT tangible

└ administration unit

└ 2 PDU seg datagram
datagram & Transport (Layer 4)

TCP - transmission control protocol

UDP - user datagram protocol

encapsulation - deencapsulation

└ traversal through the stack

header

└ ID for data

FCS - frame checksum sequence

└ detects errors - does NOT correct them

Speed - NO es lo mismo que ancho de banda

└ es dinámica, cambia a lo largo del tiempo

└ bandwidth - el max del canal

└ que tan rápido se puede mover en ese canal

└ regardless of bandwidth

Cost

└ todo lo que involucra mantener la red operando

└ separar, update, mantener, montar / preventiva

└ la red demanda recursos

└ millones de dólares / pesos

└ mal $Q_1 \Rightarrow$ en enterprise: 40-60 MDD

LAN

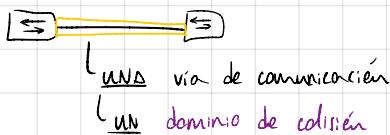
└ by definition - it IS a network

→ DHCP is actually an application

LAN components: protocols

- Ethernet
- IP
- ARP

a switch has interfaces, NOT ports



un hub es un multiconector

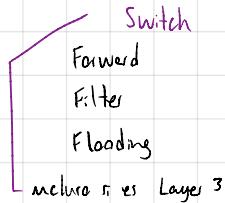
- ↳ tiene un solo col. domain
- ↳ es una sola vía de comunicación

when in doubt, manda paquetes (col. domains)

- ↳ UN enlace puede cambiar todo

- Broadcast domain -

- todos se enteran



~~Network access~~ → Data Link

Physical layer

- NIC
- physical medium

Data Link Layer

- changes de protocolos *scope for this week*
- PPP, HDLC, **Ethernet**, Frame Relay, Spanning tree, VTP, DWDM, Atom, ATM

- cada protocolo tiene su serializador

- ↳ dice que protocolo estás usando

↳ Ethernet - MAC add

- ↳ serial NO es Ethernet - es serial
- ↳ ergo, NO tiene MAC add

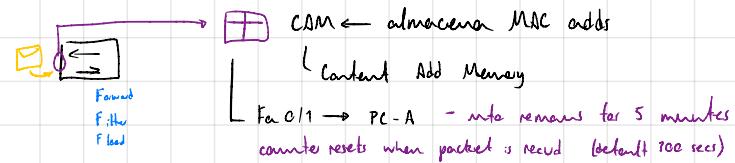
HDLC - DCE / DTE

PPP - LCP / NCP

thus, an Ethernet frame must transport a MAC add

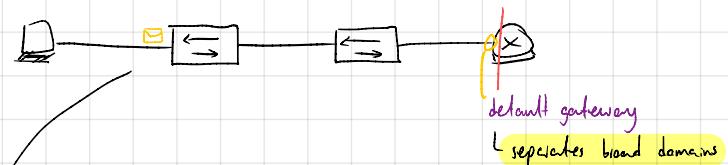
→ PPPoE manda PPP en Ethernet
↳ hacece parsear

Ethernet Frame: source & destination



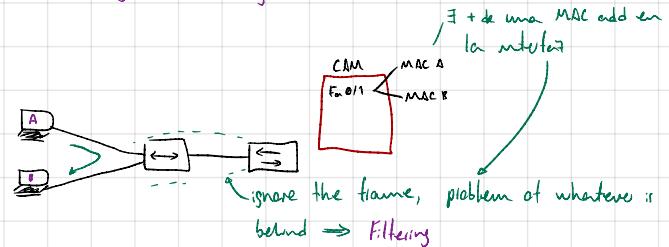
→ conoce puertos de default en todo

↳ examen si NO te dicen ⇒ assume default contig



compu responde ⇒ tiene destination

↳ ~~flooding~~ ⇒ forwarding



unicast

broadcast

multicast

IPv6 anycast

- ↳ uno al más cercano
- ↳ one to nearest point.
- ↳ one to one among many

(nodo filiando en el sigue por num v dord)

(cualquier funciona)

Layer 3: Internet / Network

→ IP protocol, OSPF, EIGRP, IMAP

↳ \exists nomás 240 protocolos IPs → 1: ICMP
(ping viaja gracias a él)

ARP es intercarga

↳ map IP add to MAC add

2: IGMP

4: IP itself

8: EIGRP

19: OSPF

Puertos / (sockets)

↳ las weas que conectan

capa transporte — capa aplicación

16 bits → cuantos aplicaciones hay (ese numero en base 10)

toda aplicación requiere un puerto

toda protocolo llaman directamente a IP

→ TCP es un protocolo IP (protocolo 6)

→ UDP, IP 17 protocol

- TFTP - puerto 69 UDP

- IP es connectionless

→ IP ↗ IP origen — origin MAC
↘ IP destino — dest MAC

> user exec mode

↳ show — display device info, except 2 show

> enable

privileged exec

↳ lul 15

config terminal

(config)#

configure...?

↳ terminal (default)

↳ 15 niveles de privilegio

s ?

word help

*show ← most used *

session system

show ?

command syntax help

Equipo: internal

Flash - Cisco IOS software
- Backup configuration

RAM - AKA running config

NVRAM - startup configuration

console cable — rollares

↳ es un rollares — RJ45 on one end

pines 1,2,3,6 — pines involved in data transmission

SWITCH

↳ all interfaces encendidas por defecto

Router

↳ todas interfaces apagadas por defecto

up status - physical

Line proto - layer 2 - frame complete

↳ all ok w/ protocol

2 ends speaking same language

→ A los ifs NO les sirve el down (yogut)

↳ NO puede haber down-up

MDIX

Ethernet Frame anatomy

8	6	6	2	46-1500	4	Bytes
Preamble	Dest MAC	Orig MAC	Type	Data	FCS	frame check sequence

↗ last byte - SOF - start of frame - 7 consecutive zeros
↳ ahí de van la trama chiquitina
↳ ready or not

ff:ff:ff:ff:ff:ff - static on CAM

↳ when no destination MAC add set / paquete NO se puede ir incompleto

01:80 - reserved for multicast

MAC add

48 bits in length — 6 bytes in length

Vendor assigned — los pone el fabricante - serial del producto por ejemplo

OUI
↳ 24
↳ who made it
↳ IEEE IANA
↳ organizationally unique identifier

→ todo lo wireless es half-duplex

L bit de paridad - canal libre pt/ transmisió

⇒ wireless es más lento que el cable

yeah, it has full-duplex-style functionality

- jamás podría ser full por el momento

- interfaces en dynamic auto - ready to negotiate

L negociaje from fastest/full to lower

best practice - no dejar nada en auto-negociación

(pero con auto (en Cisco) todo jalar)

→ we want to avoid mismatch

- Troubleshooting según Cisco -

→ 8 metodologías

L sometimes we have to combine them

- structured [3 steps] House M.D. -

- observa síntomas & signos

- bateémoslo como x

(y si no es x?)

L sabremos que no fue x, pero trataré como x

problema - una causa - NO su consecuencia

→ analizar info

L core-sabré cómo funcionan las cosas

L eliminar causas potenciales - optimizar tiempo de troubleshooting

L hipótesis → jalo / no jalo ↴

- Shoot from the hip -

→ tú intentate - sin eliminar causas potenciales

- Top-down -

→ todas las capas 0/1 7 → 1

Bottom-up

Divide & conquista

- start @ Layer 3

L IP es el que más troubleshooting tools tiene

- el ping se origina de la mitad más cercana al destino

② compare devices

- Why? (works on A, does Not on B)

- Follow the path -

- recrea el camino

- Swap the components -

- no siempre se padece tho

L madre cambia componentes en pleno vuelo

- Bloque 7: Intro to connectivity -

IP is a connectionless protocol

IPv4 - dividido en 2 partes ↴ red host
L 32 bit string

IPv4 header

DSCP - código diferenciador de servicio & Service type
└ Class Selector

TTL 255 por default

L saltos - broadcast domain

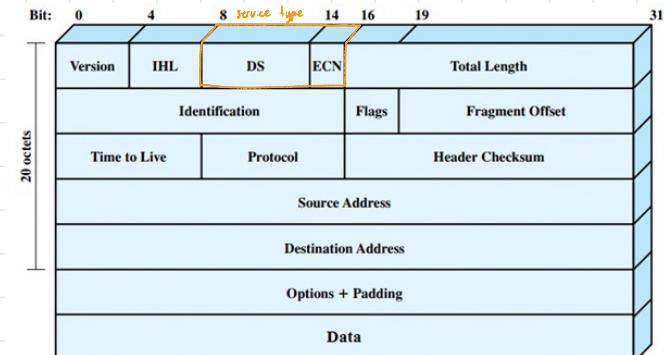


Figure IPv4 Header

Class A 1 - 127 1 - 126 ↴ Loopback testing
verifica en hardware
verifica network card works
"ping elections"
L todo el segmento reservado

Class B 128 - 191

Class C 192 - 223

Class D - multicast 224 - 239

Class E - investigación

③ decrement TTL

/ DNSs

www1 - primary DNS
www2 - secondary
www3 - tertiary

al inicio 0100 - MAC multicast !!!

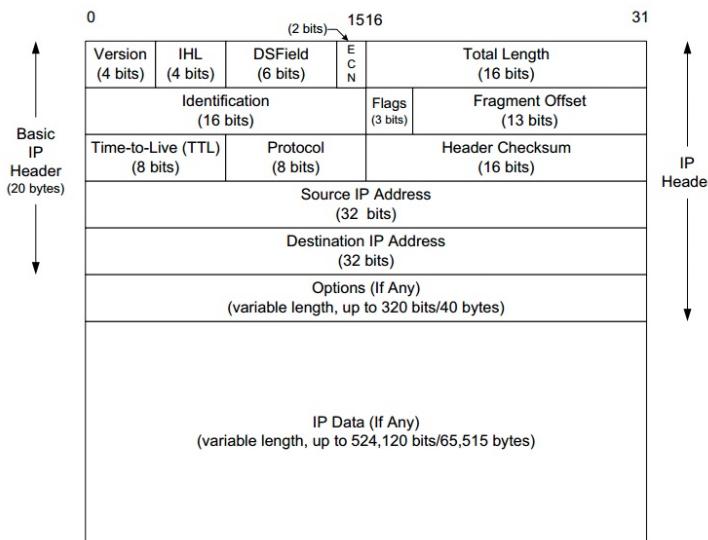
37.com
Search on 37 engines

decments TTL

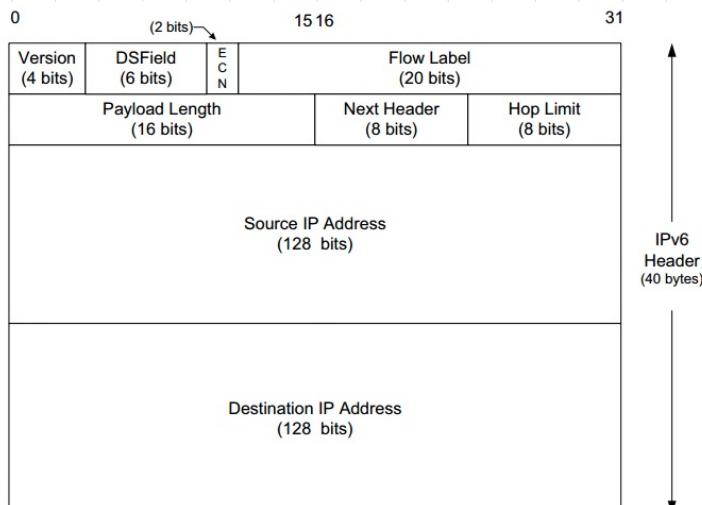
IP está orientado a la no-conexión

- only provides best-effort delivery and its service is characterized as unreliable

IPv4 header



IPv6 header



→ single area ~ multi-area OSPF

OSPF → link-state routing protocol

→ builds & maintains a topology database

- Hello packets and LSAs used for such purpose

Hello packets

- discover neighbors and establish neighbor adjacencies

LSAs → (Link-state advertisements)

- exchanged between all OSPF routers to build the topology database. ← that is used for best path selection

Note: the SPF algorithm is CPU-intensive ⇒ time it takes for calculation depends on the area size

- ↑ rationale for Multi-Area OSPF

→ Each routing protocol has a unique method for calculating route metrics (cost)

- OSPF calculates cost based on link bandwidth.

recall: two functions of a router are:

- connect multiple IP networks
- determine the best path to send packets

recall: in order for packets to be sent to a remote destination or host must have 3 settings correctly configured

- IP add
- subnet mask
- default gateway

Administrative distance

- trustworthiness of a particular route

Metric

- routers with the smallest metric to a destination indicate the best path

- Dia 2 -

IPv4 - 4 octetos, 8 bits each \Rightarrow 32 bits

- Subnetting y máscaras -

$x.x.x.y/x$ \rightarrow prefix



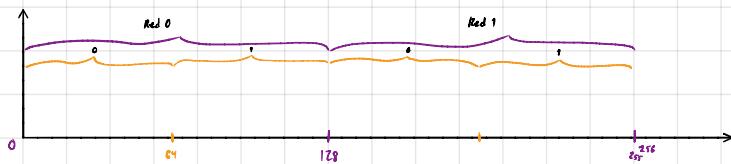
00 00 00 00	.128	}
00 00 00 00	.192	
00 00 00 00	.224	
00 00 00 00	.240	
00 00 00 00	.248	
00 00 00 00	.252	
00 00 00 00	.254	
00 00 00 00	.255	

possible máscaras de red
normal están

Indicates bit amount in network portion

→ network is / behaves as a vector

$$\angle 0 \rightarrow 255$$



→ toda el área de host en uno

↳ ID de la red en la que estoy trabajando
↳ Network ID

→ toda el área de host en uno

↳ última add antes siguiente red
↳ Broadcast (ing) ID

NO se deben de utilizar

Ejercicios

10.197.131.252/19

10.197.10.00 0011.1111.1100
area de host

Net ID 10.197.128.0

First Host 10.197.128.1

Last Host 10.197.159.254

Broadcast 10.197.159.255

Next network 10.197.160.0

pero en el examen NO hay tiempo :)

↳ técnica y práctica

$\begin{array}{r} 128 \\ + 64 \\ \hline 192 \\ + 32 \\ \hline 224 \\ + 16 \\ \hline 232 \\ + 8 \\ \hline 231 \end{array}$	10.197.231.252/22
	10.197.1110.0111.1111.1100 next: 10 21 22
	Net ID = 10.197.228.0
	F Host = 10.197.228.1
	L Host = 10.197.231.254
	Broadcast = 10.197.231.255
	Next net = 10.197.232.0

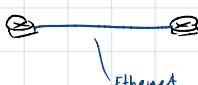
→ ↗ crea nuevos broadcasting domains

↳ ↗ es segmentar la red

divide los dominios de broadcast

↳ y crea dominios de broadcast

when in doubt, orientate traffic!



Domino de Broadcast

NO se considera domino de colisión



NO hay domino de colisión
↳ no hay MAC

↳ es un enlace point-to-point



2 de col, 1 de broad

CDP

- habilitado en all Cisco devices por defecto
- info refreshes every 180 secs (3 mins)
- local if - my int
- port ID - neighbor's if

Tabla ARP saved for 240 minutes

Lab

one way → should we static routing



sys autónome colección de redes administradas bajo el mismo dominio
(Walmart es una red)

ruta apunta a otra sys autónomo?

↳ interfaz de salida (only use here)

↳ otherwise → recursive routing

siempre ponemos el next-hop router pls

no conozco la red? — default route

↳ quad-zero, exit interface

↳ again, NO se recomienda within sys autónomo

→ equipos más nuevos NO soportan full declaration

→ tu siempre usa next-hop

TODO

Loopback

CDP

- ↳ hold timer bajando
- ↳ cada momento hace refresh
- NO confies 100% en CDP
 - device que ya no esté - 180 segundos pt que desaparezca de la tabla
 - puedes cambiar el timer (hacelos en todos)

LLDP - LL discovery protocol

- ↳ el que no es Cisco proprietary
- ↳ Linux-based ⇒ encontrar mas Linux

CDP → si se marca el tiempo cero

— no más configuras clockrate

- ↳ HDLC ??
- ↳ LLC protocol - sincrono, requiere clock rate
 - ↳ same LOS 12.5

Regla 1 de la red:

- ↳ NUNCA asumas nada

I llegó bien

. salió pero no llegó bien - si hay camino

u unreachable - busqué el unicamino pero NO lo hallé :-)

RFC 1918

- ↳ 16 bits en red al menos
- ↳ una clase B tiene 1/16 (y clase A, C, ...)
- ↳ si es 1/16 es classful

Protocolo ④ de IP → ICMP

MAC add bere - la que está en el silicon/chipset

Todo el detalle está en ~~IP~~ ^{origen IP} dest IP

El PING siempre se origina de la mt más cercana al destino

No es que no hagan ruta de retorno

↳ Es la estructura del paquete



me ahorra todo este con dynamic routing

El ping pregunta qué...? mas no qué??

loop de intero

balanceo de carga

2 equal paths

- ACL -

→ su finalidad es negar

↳ debe admitir algo

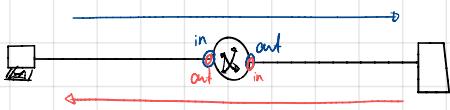
veremos standard & extended

standard — "todos los hombres son iguales"

↳ only verifies origin | numbers 1-99 / 1300-1999

extended — "ademas en US"

↳ src, dest, content | numbers 100-199 / 2000-2699
↳ plus range extended



→ jerárquica y se revisaría de arriba a abajo

↳ no tiene statement limit

↳ on Cisco gear, >5000 statements

↳ el ↳ impresa el inappropriate behavior

↳ los otros desde 1500

→ ACL must be capable of optimizing

access-list # permit
access-list # deny

de lo particular a lo general

por defecto TOSC está negado

↳ must ↳ al menos un permit

std debe colocarse lo más cerca al destino

extended lo más cercano al origen

every statement by default enumerated 10 by 10

IC, TC, IC, 4C

gap to add intermediate statement
if ever required

resequence - reenumerar las sentencias - todos siguen guardadas

Std ACL solo trabajan con protocolo IP

extended diversos protocolos

↳ filtra protocolo

permit TCP x.x.x.x y.y.y.y eq 23

permit Frank to CEM eq 23

wildcard: bits that CAN change (and do change)

→ el nombre de la ACL puede ser un número

↳ standard - 100 ↳ reserved for extended

↳ podría llamarse '50' e.g.

→ la vdd, ↳ muchos! tipos de ACLs

dinámico, time-based, ... - .

no access-list #

↳ aplica a todas las sentencias en la 1

↳ siempre backup antes de hacer cambios

→ outbound ACL - primero todo el ruteo (procesamiento)

↳ int - tienen ACL? → test para cada statement

↳ si, que se vayan
desactivado

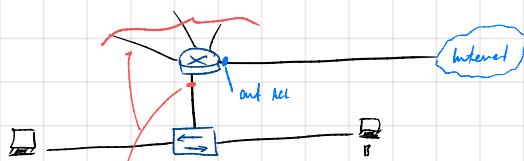
→ ACLs can be applied to in & out more

↳ only one ACL per interface

"only one ACL per protocol, per direction and per interface is allowed." - "Important" en la diazo

→ the default wildcard mask is 0.0.0.0 (standard only!)

- recall: closest to destination



si pongo una IN (wrange), compromete acceso a otros servicios

sólo quiero que host B NO acceda a Internet

↳ conviene usar and ACL

→ ACL and wildcard exercise

172.16.144.0/22

primero checar que sea una red

/
 1 0 0 1 0 0 | 0 0 . 0 0 0 0 0 0
 si es una red \Rightarrow los puedo filtrar

wildcard: 0.0.3.255 / los bits que si pueden cambiar

→ la wildcard es un elemento MUY poderoso

10.10.128.131 0.0.0.128 - optimiza la ACL en un 50%
 (Resumen)

0.0.0.0 - nada puede cambiar

i.e., un host, niega a un host
 igual palabra reservada host

255.255.255.255 any

- Configuring named ACLs -

sólo lo ponemos cuando es necesaria o extendida

(config)# ip access-list standard solo-tamitos
 [conf std-nacl]# permit 10.1.7.0 0.0.0.255 \rightarrow match primera octeta

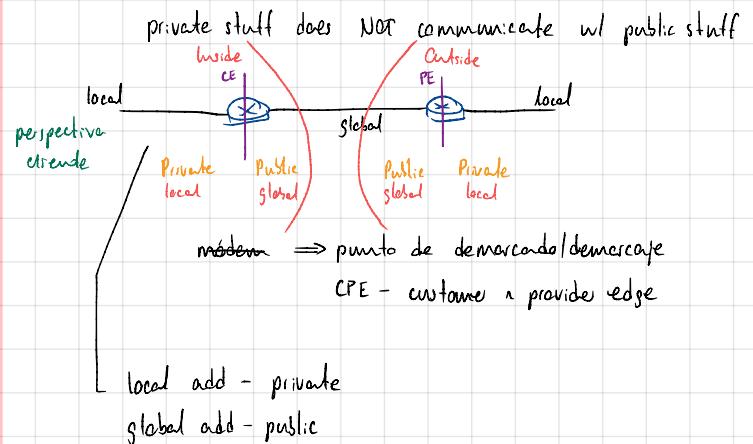
si es extendida \Rightarrow poner protocolo en el statement

⑩ nombrada \neq numerada

- Enabling connectivity -

- NAT -

IPs classified in private
 public



Types of NAT

Static nat one-one

Dynamic nat many-many

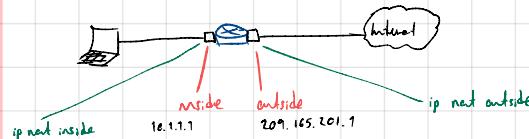
PAT many-one address mapping

→ NAT requiere el uso de una ACL

✓ no requiere otras reglas
 static NATting vincula qd permite

per cada pvr add, requiere una add publica
 pvr int - inside
 pub int - outside

construir la regla de NAT: 20



Class A private — RFC 1918 (1)
 10.0.0.0 - 10.255.255.255

Reservadas

A: 127.0.0.0
 B: 169.0.0.0

Link-local

Class B private
 172.16.0.0 - 172.31.255.255

Class C private
 192.168.0.0 - 192.168.255.255

→ intero - comunicar lo privado con lo público
└ por eso la interfaz que va a Internet es una static default

→ marcar qué es adentro / afuera

└ en la red "puede salir para adentro"

tabla de traducciones - lo más importante en NAT

→ NAT no deja un registro

└ deba regresar como scd

└ si NO → alguien otro se paquete

→ traducción uno-a-uno

ip nat inside ← hard-type, always!

ip nat inside source static 10.1.1.2 209.165.201.5

afuera eres una cosa, adentro eres otra

Translation table

└ lo q te permite a la info regresar

→ NATEo estático NO es escalable

company: 80%
80% sale a internet

20% within enterprise network

NATeo dinámico

pool de direcciones

ip nat pool MY-Pool start add end add netmask count
range

cuántas personas pueden salir a Internet al mismo tiempo

Configuring Dynamic NAT

R(config)# access-list 1 permit 10.1.1.0 0.0.0.255

R(config)# ip nat pool MY-Pool 209.165.201.5 209.165.201.10 netmask
255.255.255.240 hasta 6 pueden salir a Internet al mismo tiempo

pool de públicos
dinámico - idea de que NO todos usaban el servicio al mismo tiempo
└ today's needs? → no-nh

└ también tenemos ints inside + outside

inside - translation & adentro ⇒ afuera

hacemos ACL para llamarla

source list llama ACL

- pero hay todo el mundo quiere salir al Internet

└ o sea este ya no

└ periodo breve de conectividad (ahí funciona)

→ first available is assigned

→ decir qué es inside / qué es outside

- Port Address Translation (PAT) -

└ (NAT overloaded)

→ si decrementa performance

└ es lo que hay

- hacer lista

- marca int m sub out

- ip nat inside source list 1 int G0/0/1 overload

también puedes hacer dynamic PAT

→ dirección disponible hasta que se sobrecargue

- Dynamic PAT -

→ hacer un pool y comando overload :P y ya +

- Layer 2 -

- VLANs and trunks -

Implementing scalable medium-sized networks

Access Layer en 3-tier

└ redes convergentes aquí

Distribution Layer

└ distribuye los recursos de la red

provides:

- Routing & packet manipulation
- Scalability

≡ 2 svcs qd NO puede querer

→ el cliente requiere una IP - request to DHCP

when PC se quiere conectar por primera vez a la red... → discover broadcast

IP origen	0.0.0.0]	No las puedo eliminar de la red
IP destino	255.255.255.255]	(muy necesario)
MAC origen	a a a a a a]	necessary / critical for this
MAC destino	ff:ff:ff: ff:ff:ff	broadcasting	

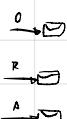
DHCP server está instalado hasta core

└ habrá rutas que acceder al service al user

└ actualmente están en Distribución

Dominios de Broadcast virtuales ⇒ VLANs

└ agrupamiento lógico



VLANs

└ dominios de broadcast

└ compromiso 1 device ⇒ VLAN compromised

└ instead of whole net

det' - subdominio de broadcast propagando en L2

Front

det' - "un vil cable"

VLAN 0?

└ can be created

└ only some elements support it

└ members /
└ don't x

NO switch can create > 4094 VLANs - NO more bits

trunk - multiples VLANs → no default

└ tagged traffic & native VLAN traffic

Nativa - es la de control y admán

└ NADA conectada

Ranke-on-on-stick (ROHS)



hex(tag) - 4 bytes = 32 bits

└ se agrega al Ethernet frame

└ justo después del source address

ISL - ni Cisco lo usa - agranda tramas

└ fragmentation de tramas

└ inter-switch-link

switchport trunk encapsulation dot1q

switchport mode trunk

└ verify mtu slow mt fact1 switchport

└ verify mode operational → de man nat
└ mtu fact1 switchport

test

└ show interface interface switchport

└ la buena

DTP

trunk puede operar en 3 modos

Auto - mtu operación claramente diga q

(dynamic) Descripción - ver access? - ser access
pero siempre habrá de negociar tramas

switch mtrs per detecto seu dynamic auto

→ manual configuration is recommended

switchports que NO vayan a way

↳ metelles a una VLAN arbitaria ⇒ Muestra la VLAN

↳ mantiene en la red

DHCP

asigna dinámicamente addrs thru DCRS

Data:

Discover

Offer

Request

Acknowledge

server fa da add ⇒ se vuelve tu default gateway per detecto

Default route

↳ default gateway, es el

DHCP never arrienda IP odds ⇒ lease

primero contiguous excluded odds ⇒ Range

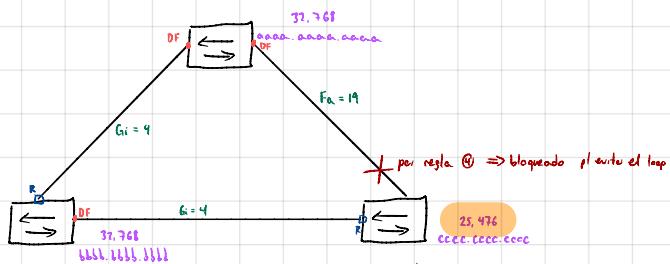
↳ lo que no debe renover su direccionalmente IP

default route must match physical int

10.10.10.1 for p1

↳ card 1:1 ⇒ assign if

- STP -



escogemos un device

root

↳ lowest bridge ID

↳ priority, MAC add

↳ default 32,768

↳ 0 - 65,535

* este es core topic

MAC sólo importa si: Pri: res la misma

primero checa pri, luego MAC

→ el tráfico va hacia el root

- el resto de los devices se llaman Non-root

→ todo non-root sw deberá tener un root port

root port

↳ camino más corto al root

↳ hay un cost ⇒ path cost

Eth 100

Fan 19

Gig 4

10 GbE 2

40 GbE 2

100 GbE 2

y ningún costo puede ser menor que 2.

↳ exit-int del best path = root port del Non-root device

- el device escoge el root port

Resolviendo any spanning tree

1) Find root - menor BID

2) Find Root port & non-root

↳ sólo puede \exists 1 por device

3) cada dominio de colisión debe tener un design. port y
estos van forwarding (D.F)

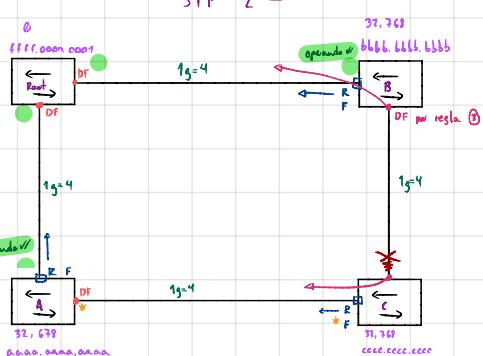
↳ todo root port se conecta a un despert que está en
forwarding i.e., Root \Rightarrow D.F.

4) todo lo demás se bloquea

↳ si perdemos ruta, el puerto bloqueado se desbloquea

↳ "necesito hablar con él"

	Role	Status	
Root	Designated	Forward	"el root es chilango" (DF)
Non-Root	Root	Forwarding	
Non-Root	Alt (rescate)	Blocking	



* si el pathcost es igual \Rightarrow desempate de alguna forma

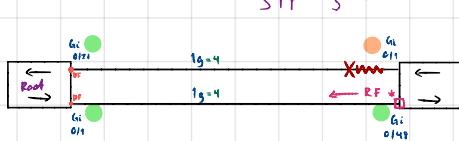
\hookrightarrow Menor BID / sender
 i.e. su vecino - lo necesita para llegar a Root

recall: Non Root \hookrightarrow

\hookrightarrow Root port = 1) Pathcost

2) Menor BID del Sender

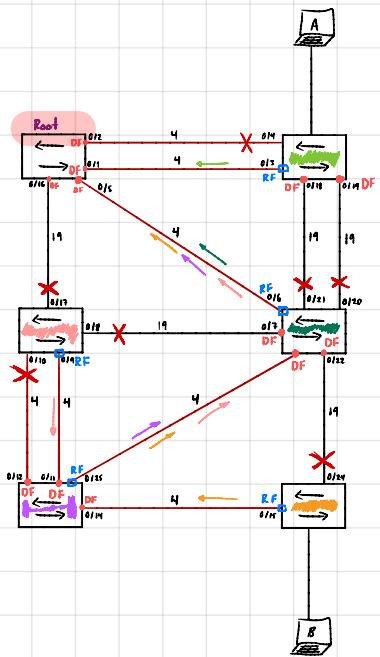
\hookrightarrow el que te está diciendo
 "ven conmigo"



3) Menor port-ID del sender*

"el root es chido" (DF)

François STP challenge :-)



Resolviendo any spanning tree

- 1) Find root - menor BID
- 2) Find Root port & non-root
 - ↳ sólo puede $\exists 1$ por device
- 3) cada domino de colisión debe tener un design. port y estos van forwarding (D. F.)
 - ↳ todo root port se conecta a un despert que está en forwarding i.e., Root \rightarrow D.F.
- 4) todo lo demás se bloquea

↳ si perdemos intera, el puerto bloqueado se desbloquea

↳ "necesito hablar con él"

etiquetamos un device **Root**

↳ lowest bridge ID

↳ priority, MAC add

NonRoot \Leftrightarrow

↳ Root Port = 1) Pathcost

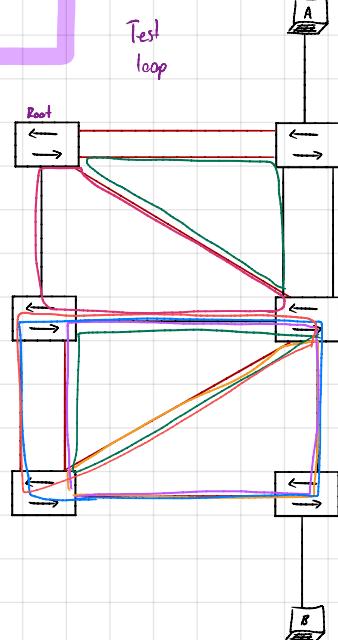
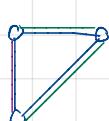
2) Menor BID del sender

3) Menor port-ID del sender

↳ default 32,768

↳ 0 - 65,535

	Role	Status
Root	Designated	Forward <small>challenged DF</small>
Non-Root	Root	Forwarding
Non-Root	Alt (elected)	Blocking

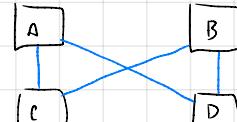


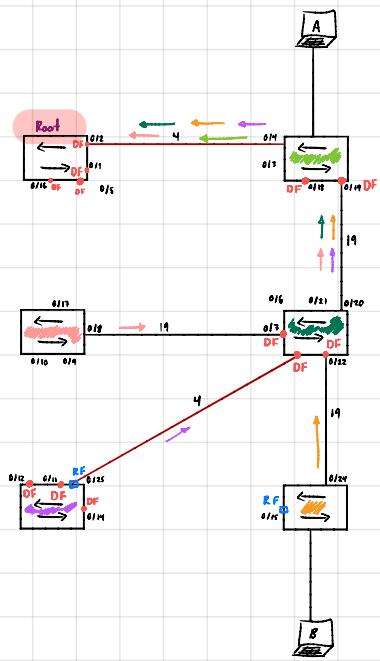
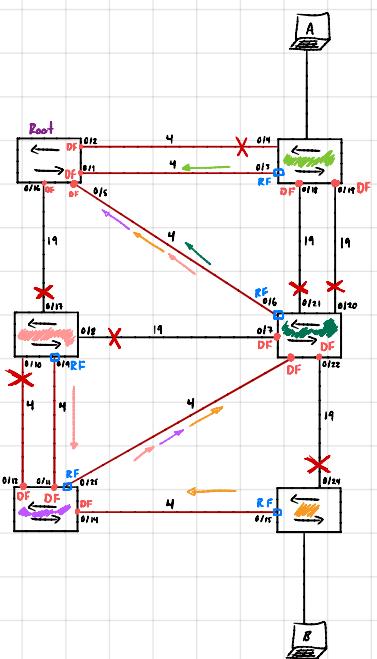
More test loop

- 1 A, B, C, D ✓
- 2 A, C, B ✓
- 3 A, C, D ✓
- 4 A, D, B ✓
- 5 D, B, C ✓

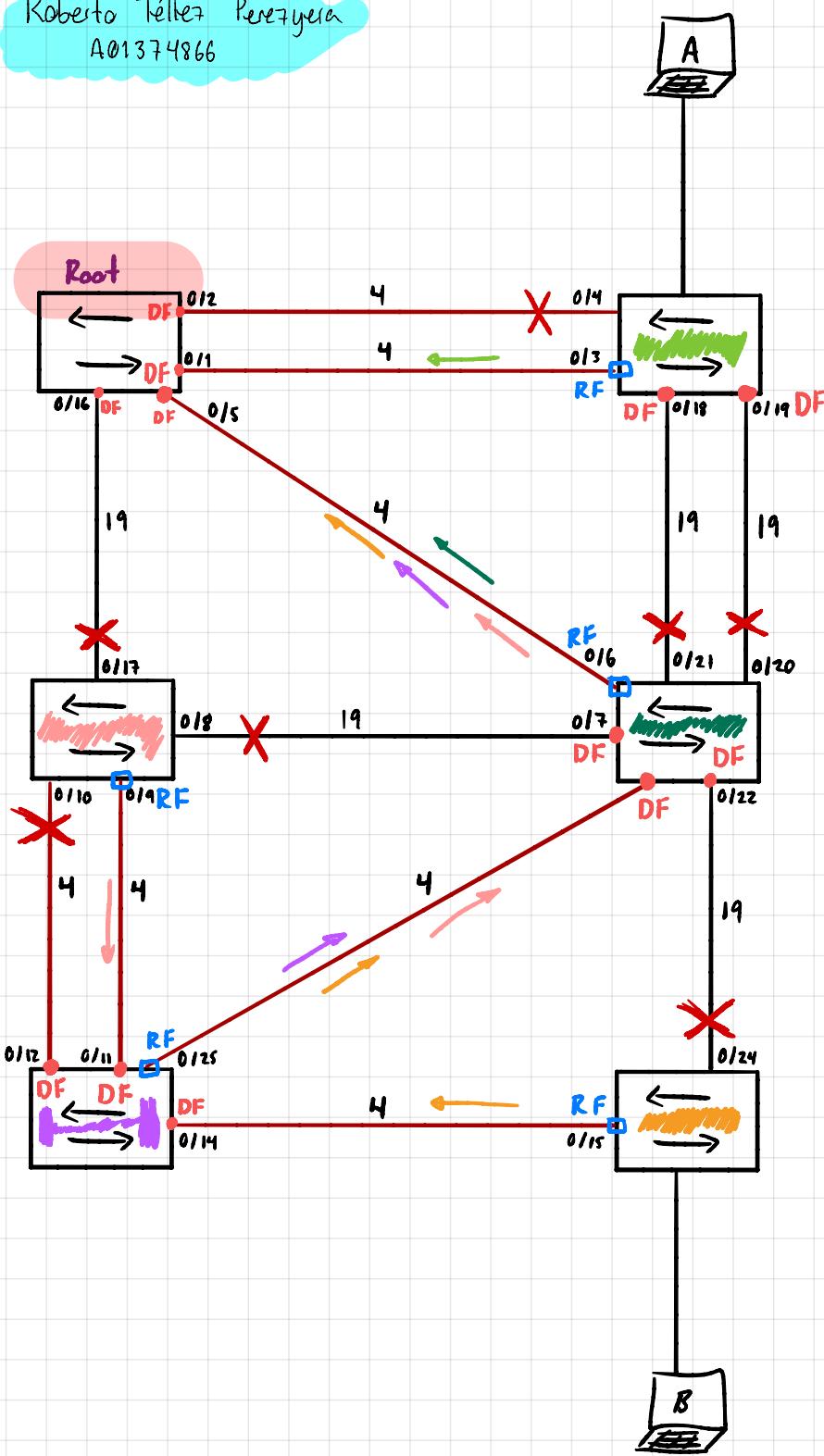
- 1 A, B, C, D ✓
- 2 A, C, B ✓
- 3 A, D, B ✓

- 1 A, B, C, D ✓





Roberto Téllez Pérez yera
A01374866



Day 4

- EtherChannel -

- link multiplication \Rightarrow loop prevention critical
 ↳ some ports disabled

- optimize spanning tree is a good idea

↳ avoid waste of infrastructure

↳ blocked links

per-VLAN spanning tree

802.1Q# spanning-tree vlan 30 root primary

- topology todo en verde

↳ se optimizan los enlaces y el flujo de tráfico

↳ para algunas VLANs

↳ más enlaces \leftarrow ^{forward} block

EC agrega a todos los enlaces y lo hace ver como un solo link

↳ crece bandwidth \leftarrow only expect compromised if a single link fails

2 protocolos

LACP

↳ standard protocol (IEEE)

↳ máximo 16 channels agrupados

↳ 8 active, 8 standby

LACP



para que PC se configure, todos los links deben ser iguales

↳ fast, Gig, trunk

↳ duplex, speed, ...

→ mts unidas en un solo PC

show etherchannel summary

I - standalone

↳ diferente config en cada extremo

P - in PortChannel

PAgP (Part Aggregation Protocol)

↳ Cisco proprietary protocol

↳ max 8 channels agrupados

Balanceo:

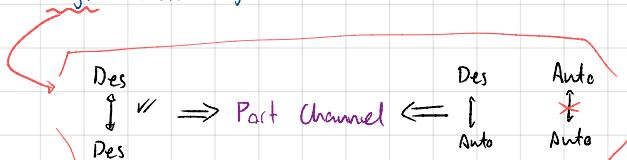
4 canales \Rightarrow 2 unidades de carga

2 canales \Rightarrow 4 unidades de carga

trunk formed in 3 modes

auto, desirable, ...

↳ PAgP funciona igual



"Port Channel" == "Ether Channel"

↳ para Cisco

- Ruteo entre VLANs -

RCAS

↳ physical if w/ subifs

only limit in the network

↳ created all the configura

puedas tener as many as I want

Tranbleshotting

Patchchannel OK?
Port -- correct?

→ Show VLAN

↳ traeves las 4?

→ Show spann

↳ que sea root sólo de los que debe
S1 ⇒ VLAN 1, 10 only!

20 root

40 root

✓

↳ en todos S1

no spanning-tree vlan 1, 10, 20, 30, 40

↳ que el 10 resuelva solo

PPP chap PPP pap

- Seguridad -

(cont) # enable password CISCO

ifm cisco password crackes
7 pass
5 sec
overrides

disable ⇒ regresa al modo anterior

"cifrado", NO "encriptado"

líneas de vty

Switch: 16

Routers depende - proteger todos

line vty 0 ? → cuantas líneas tiene este?

login → persona que esto funcione

↳ si no se jala

→ crea una DB de usuarios

username ~~~ password ~~~
username ~~~ secret ~~~

(vty) login local ← llama a user DB

fuerza de banda - vía consola

admin en banda

necesaria al estar conectado a una red

también login local van line con 0

username cisco privilege 15 secret cisco

- SSH -

- router debe de llamarse cualquier forma

excepto fábrica ("Roubo")

- routers deben pertenecer a un dominio

- certificado de seguridad

↳ al menos 768 bits en la clave para Version 2

public key infrastructure

sh crypto key mypubkey rsrc

ssh -l cisco 192.168.1.100.1

\login

⇒ banners tienen que ser agresivos

motd

↳ puede contener NDA o mensaje secreto

↳ fines legales

↳ puede decir lo que sea

banner login - fines legales

↳ el agresivo

any any

↳ origen ↳ destino

acc-group - phys int

acc-class - virtual int

- Port security -

switchport port-security - enables Port Security on interface

↳ van al final (la convención)

remember: interfaz debe estar en access mode

switchport port-security maximum 1

2 con teléfono IP

as many as devices you have

protect
restrict*
shutdown default
Log

switchport port-security violation

↳ shutdown default

MAC se almacena en la tabla

↳ es el backup

↳ por si el sw pierde power

MAC addresses

↳ se almacenan en la tabla de direcciones

↳ #show mac address-table

↳ es el backup

↳ por si el Switch es reiniciado

- RIP -

dynamic routing protocol

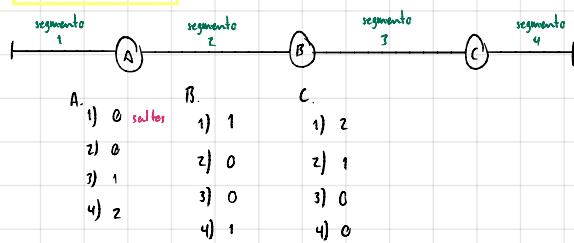
es lento en su convergencia

Hello = 30 seconds

Hold-down = 180 secs

Flush = 240 secs

[hops / 120]



3 reglas de R1:

→ CI (count to infinity)

↳ loop de numero de saltos

↳ solution: red a 16 hops es inalcanzable

ya NO se
considera alcanzable

15 - 16

⊗ ⊗

→ Split horizon

↳ NO puedo publicar redes publicadas por el otro

↳ evitar situación anterior (loop)

→ PR (poison reverse)

↳ notifica que una ruta se perdió

↳ le va a regresar la llamada

↳ poca tención que transcurris 180 secs

↳ termina flushando una red que cree que perdió

RIP es classful - publica toda la clase

↳ versión 2

↳ opción de verlo NO classful en la routing table

→ Auto-summary

↳ "resume" todo a una dirección classful

↳ usar no auto-summary

↳ maneja más redes

↳ se incluyen todas las subredes y sus máscaras

classless

- end of day 4 -

Day 5

toda protocolo vector-distance es classful.

↳ NC, RIPv2 is NOT classless

Link-state protocol

crea 3 tablas

↳ neighbors, topology, routing table

buse de inter

OSPF

↳ gran capacidad de crecimiento

↳ organiza en áreas

↳ NC more than 50 routers per area (recommend'd)

link

state - relacion el el vecino a través del link

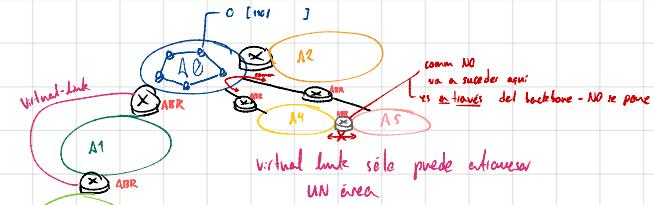
sys autónoma

toda el sys de áreas que yo administro

debe ↑ un área cero ⇒ backbone

↳ debe permitir comunicación a otros áreas

TODA área debe estar conectada al área 0



Hello packets

↳ periodically sent to multicast add 224.0.0.5

Router ID
Hello/dead interval*
Neighbors
Area ID*
Router priority
DR IP add
BDR IP add
Authentication data*
Stub area flag

* must match

ampliamente usado ⇒ gratuito

Router ID

L no nombre colocado?

L router toma nombre int loop \Rightarrow es estable

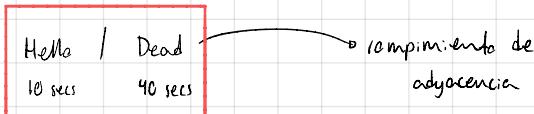
L multiple? IP mas alta

L vez IP mas alta among int

L numero de 32 bits en 8 octetos

L NO es una IP, es un nombre

Cuidado con duplicados \Rightarrow degenar.



Area ID - Binho del area (CEM)

Priority ① - 255

Designated router - el q controla traffic flow

L todos se deben comunicar con él

L el más importante del area

OSPF uses two multicast addresses

224.0.0.5 - el resto

224.0.0.6 - DRs

L RIP - multicast 224.0.0.9

BDR - backup - el segundo mejor

L selected according to: 1) priority

2) highest RID

NO DR, BDR? \Rightarrow DR OTHER - es mi boder

OSPF supports 3 authentication types

0 - sin autentic.

1 - aut. en plain text

2 - MD5 (hashing del secret)

why? \Rightarrow verify $\otimes_i \in \text{Area}_j$

Stub area flag

L separated from the group



no necesita accederse a los routers de todos

L esta área sólo tiene y necesita una default static route (stub)

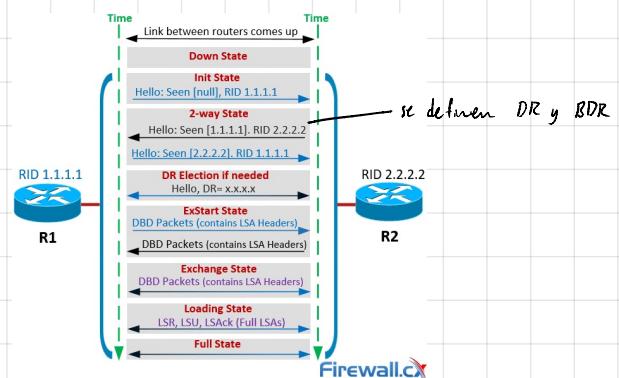
goal: reduce routing table size

L reduce router workload

← eso fue el Hello packet - el más importante

7 estados pl former relación c/ los vecinos

down, init, 2-way, ex-start, start



ex - If art es crucial \Rightarrow compara MTU, has to match

L match?

\hookrightarrow Exchange (base de datos)

LSAs - Link-state acknowledge (11 diff types)

↳ Loading state \rightarrow carga-registro de información

↳ Full - lista, ya sabemos todo de todo

-SPF-

Dijkstra Algo \Rightarrow SPF tree

3 5 types of OSPF packets

Hello discovers + maintains neighbors
 DBD
 LSR
 LSU
 LSAck

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	DBD	Checks for database synchronization between routers
3	LSR	Requests specific link-state records from router to router
4	LSU	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types

Hello y Ack - NO llevan Ack

router ospf <process-id>
 network (net-add) (wildcard-mask) area (area-id)
 o directly over the interface
 (cont if) ip ospf (process-id) ... (?)

adyacencia en OSPF

MATCH - Area ID
 - Hello Dead Interval } test
 - Network
 - Authentication
 - Stub

sh ip protocols
 sh ip net br

path cost as a metric

anything > 100ms = 1
 (⇒ modify costs manually
 interface bandwidth)

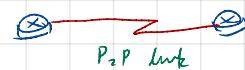
multi-area ⇒ incluir ABRs

01A [110/]

en redes P2P NO hay DR, BDR

↪ están todos los de la mano

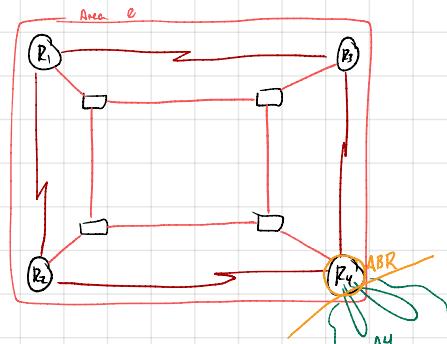
↪ $P_{ri} = \emptyset$



Designated router por área

↪ tantos como segmentos de red tengan en el área

↪ dom. broadcast



Distancia ⇒ todos los paths

↪ same destination, different paths

→ cuando el anfitrión vecinos vay a tener

sh ip ospf nei:

sh ip ospf interface

sh ip proto

sh ip ospf

sh ip ospf database

↪ LSAs - hay más, veremos 3

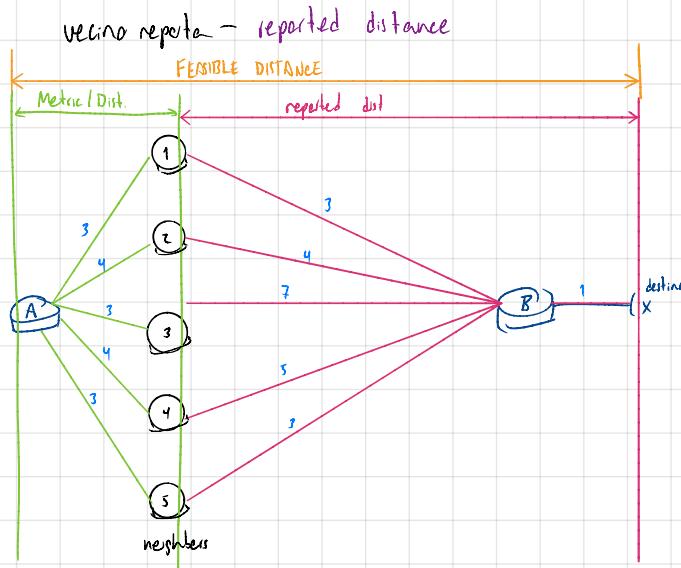
LSA 1 - Router

LSA 2 - Network → DR

LSA 3 - Summary - into ABR

- EIGRP -

- proprietary de Cisco
- es el mejor $\Rightarrow DA = 190$
- métrica compuesta
 - ↳ K values



FD Es de mi métrica y lo reportado

$$\text{Metric} + \text{RD} = \text{FD}$$

R ₁	3	4	7
R ₂	4	5	9
R ₃	3	8	11
R ₄	4	6	10
R ₅	3	4	7

3 tipos: de...

- neighbors
- topología - possible routes to X
- ruteo

Algoritmo DUAL - diffusing update Algo

successor: ruta al menor FD

↳ puede \exists multiple successors \Rightarrow load balancing

- The golden rule -

si el RD es < actual FD del successor,

↳ esa ruta es un feasible successor \Rightarrow backup

↳ backup también se instala en topo-table

- bandwidth \Rightarrow K1

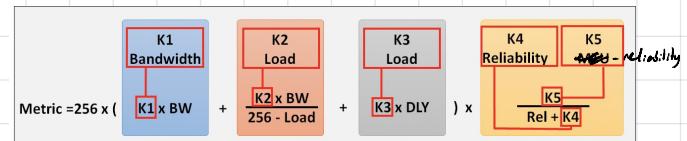
- delay \Rightarrow K2

K2 - carga

K4 } reliability - ambas son reliability

K5 }

↳ NO es el MTRU



por defecto load \wedge reli: set tc 0

K values: 0 - 255

NO se predice power today en 0

K₁, K₃ = 1
bwth load

→ en EIGRP le interesan los K-values

→ los 2 routers deben pertenecer al mismo sys autónomo

→ OSPF es classless — con máscara
classful - toda la clase

→ EIGRP dice el orden en q se encendió el vecino
↳ derecho de antigüedad

topo-table muestreo \leftarrow ^{succ} _{feasible succ}

reported distance se mide con los K values

former output \leftarrow [FD / RD]

show ip eigrp topology

nos muestra todo
(usar para subtletas)

NO se predice ve métrica n: DA

↳ PERO \Rightarrow a FD restale RD

FD - RD = Metric (si te la preguntan)

→ estrictamente menor-que

load balancing

- IPv6 -

unequal cost load balancing

modify variance \Rightarrow set to default: 1

L can reach up to 128

→ interfaces w/ less bandwidth can carry smaller packets

var multiplication * FD

caminos por donde van los paquetes tienen que ser FS

EIGRP es clásico (?)

hace las redes clásicas

en el test se contiguos

El ~ NC publica su RID

L si ve IP's

hablan del mismo vecino pero en lugares diferentes

all-links

(teas / repeated)

L \leq Feasible